Linux version of AvosLocker ransomware targets VMware ESXi servers

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)**

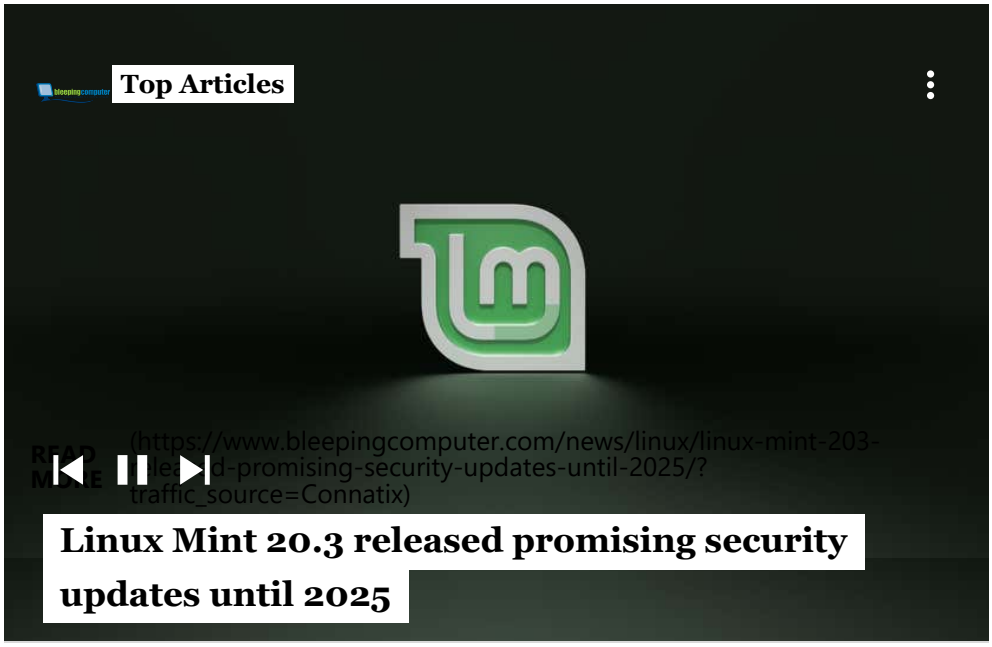
January 10, 2022 04:09 PM **0**

AvosLocker is the latest ransomware gang that has added support for encrypting Linux systems to its recent malware variants, specifically targeting VMware ESXi virtual machines.

While we couldn't find what targets were attacked using this AvosLocker ransomware Linux variant (https://twitter.com/ChristiaanBeek/status/1480551019310469120),

BleepingComputer knows of at least one victim that got hit with a $1 million ransom demand.

Several months ago, the AvosLocker gang was also seen advertising its latest ransomware variants, the Windows Avos2 and AvosLinux, while making a point of warning affiliates not to attack post-soviet/CIS targets.



"Out new variants (avos2 / avoslinux) have the best of both worlds to offer: high performance & high amount of encryption compared to its competitors," the gang said (http://twitter.com/pancak3lullz/status/1454105776759377925).

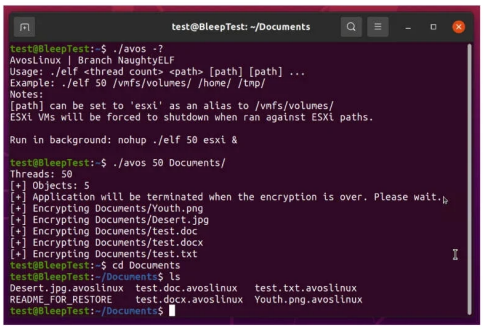
ESXi VMs terminated before encryption

Once launched on a Linux system, AvosLocker will terminate all ESXi machines on the server using the following command:

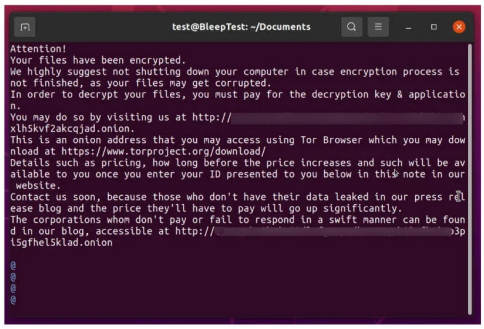
```
esxcli --formatter=csv --format-param=fields=="WorldID,Dis
playName" vm process list | tail -n +2 | awk -F $',' '{sys
tem("esxcli vm process kill --type=force --world-id="
$1)}'
```

Once it starts operating on a compromised system, the ransomware will append the .avoslinux extension to all encrypted files.

It also drops ransom notes asking the victims not to shut down their computers to avoid file corruption and to visit an onion site for more details on how to pay the ransom.



AvosLocker Linux variant in action



AvosLocker ransom note

Security researcher MalwareHunterTeam told BleepingComputer that AvosLocker began using the Linux encryptor starting in November 2021.

Ransomware's switch to Linux

AvosLocker is a newer gang that first surfaced during the summer of 2021, calling for ransomware affiliates on underground forums to join their newly launched Ransomware-as-a-Service (RaaS) operation.

The move to target ESXi virtual machines aligns with their enterprise targets, who have recently migrated to virtual machines for easier device management and more efficient resource usage.

By targeting the VMs, the ransomware operators also take advantage of easier and faster encryption of multiple servers with a single command.

Since October, Hive ransomware started encrypting Linux and FreeBSD systems (https://www.bleepingcomputer.com/news/security/hive-ransomware-now-encrypts-linux-and-freebsd-systems/) using new malware variants, within months after researchers spotted a REvil ransomware Linux encryptor (https://www.bleepingcomputer.com/news/security/revil-ransomwares-new-linux-encryptor-targets-esxi-virtual-machines/) targeting VMware ESXi VMs.

Emsisoft CTO Fabian Wosar (https://twitter.com/fwosar) told BleepingComputer that other ransomware gangs, including Babuk, RansomExx/Defray, Mespinoza, GoGoogle, DarkSide, and Hellokitty, have also created and used their own Linux encryptors.

"The reason why most ransomware groups implemented a Linux-based version of their ransomware is to target ESXi specifically," Wosar explained.

HelloKitty and BlackMatter ransomware Linux variants were also discovered in the wild by security researchers in July (https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/) and August (https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/), further confirming Wosar's statement. The Snatch and PureLocker ransomware operations have also been observed using Linux encryptors in the past.

You can find more info on AvosLocker ransomware and what to do if you get hit by this ransomware family in our support topic (https://www.bleepingcomputer.com/forums/t/754311/avoslocker-ransomware-avos-support-topic/).

Related Articles:

Ransomware gang coughs up decryptor after realizing they hit the police (https://www.bleepingcomputer.com/news/security/ransomware-gang-coughs-up-decryptor-after-realizing-they-hit-the-police/)

Shutterfly services disrupted by Conti ransomware attack (https://www.bleepingcomputer.com/news/security/shutterfly-services-disrupted-by-conti-ransomware-attack/)

AvosLocker ransomware reboots in Safe Mode to bypass security tools (https://www.bleepingcomputer.com/news/security/avoslocker-ransomware-reboots-in-safe-mode-to-bypass-security-tools/)

Conti ransomware uses Log4j bug to hack VMware vCenter servers (https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/)

TellYouThePass ransomware revived in Linux, Windows Log4j attacks (https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-revived-in-linux-windows-log4j-attacks/)